10. Safety Integrity Level (SIL)

Definitions

- **Risk**
  - **A combination of both incident likelihood and its severity**
- **Basic Process Control System (BPCS)**
  - **Control equipment and system which installed to regulate normal production functions (DCS, speedtronic, etc.)**
- **Safety Instrumented System (SIS)**
  - **System consisting of one or more Safety Instrumented functions whose purpose is to take the process to a safe state when predetermined conditions are violated**
- **Independent Protection Layer (IPL)**
  - **System or subsystem designed to reduce the likelihood or severity of the impact of an identified hazardous event by a large factor (10 times or more)**

Definitions (Cont'd)

- **Probability of Failure on Demand (PFD)**
  - A value that indicates the probability of a system failing to respond to a demand

- **Safety Integrity Level (SIL)**
  - One of three possible discrete integrity levels of each Safety Instrumented Function (SIL1, SIL2, SIL3)
  - Defined in terms of Probability of Failure on Demand (PFD)
  - Used by the industry to specify the design requirements of SIS

- **Risk Reduction Factor**
  - Reciprocal of PFD

Methodology for SIL study

- ‘C&E’ forms the guideline for scope of SIL study
- Identify and record the hazards of the process (from HAZOP) as ‘Worst Consequence’ and ‘Consequence rating’ (severity) of hazardous event(s)
- Evaluate the ‘likelihood’ for each ‘cause of the initiating event’
- Identify existing layers of protection for the identified event for each ‘cause of the initiating event’
- Evaluate the effectiveness of existing and additional recommended layers
- Determine the number of additional layer ‘’if required” to reduce the risk to “Tolerance Frequency Goal” else, “park” for later resolution
- Review the inspection and test frequency for each system that forms a layer of protection (during validation–phase-2)
- If a SIS exists or is required, determine the SIL (phase-2)

Safety Integrity Levels

Safety Integrity Level	Probability of failure on demand per year (Demand mode of operation)	Risk Reduction Factor
SIL 4	$>=10^{-5}$ to $<10^{-4}$	100000 to 10000
SIL 3	$>=10^{-4}$ to $<10^{-3}$	10000 to 1000
SIL 2	$>=10^{-3}$ to $<10^{-2}$	1000 to 100
SIL 1	$>=10^{-2}$ to $<10^{-1}$	100 to 10

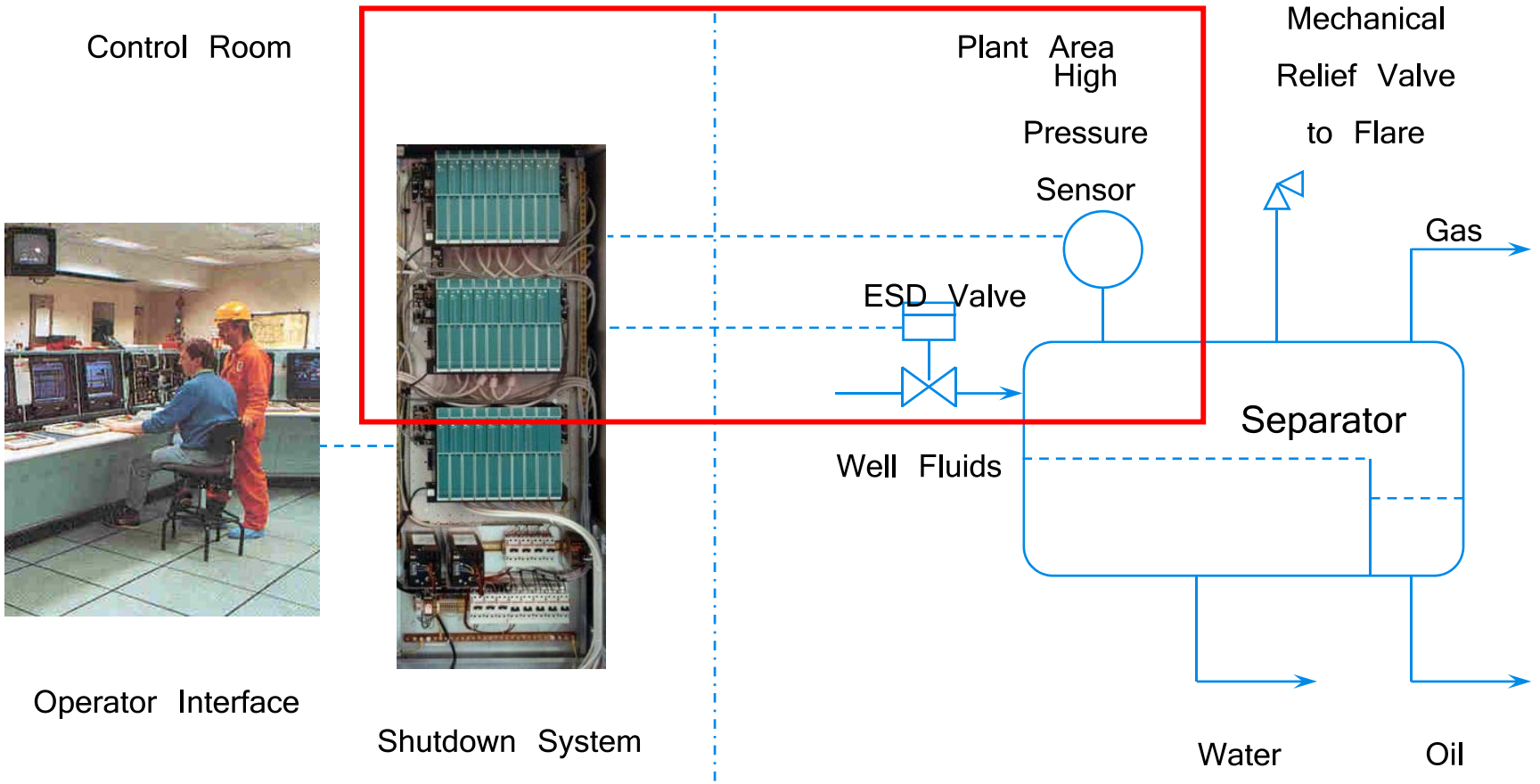
Purpose of SIS / SIL Workshop

- Inform about safety instrumented systems and safety integrity levels
- Inform about why we do SIL assessment
- Learn how to ensure that an installed system can meet a given integrity level
- Support the project commitment to high standards of safety and environmental performance

SIS/SIL Workshop Agenda

- Introduction and Safety Briefing – XYZ
- Session 1 – Background, SIL Risk graph and LOPA
- Session 2 – Example of SIL assessment using risk graph
- Session 3 – LOPA and example of SIL assessment using LOPA
- Session 4 – Quantified assessment, Reliability, IEC 61508/61511 overview
- Session 5 – How to meet a given integrity level
- Session 6 – How to meet a given integrity level, continued
- Session 7 – Valve partial stroke testing, Robustness to spurious trips, Operational requirements
- Session 8 – Next Steps

Example Safety Instrumented Function



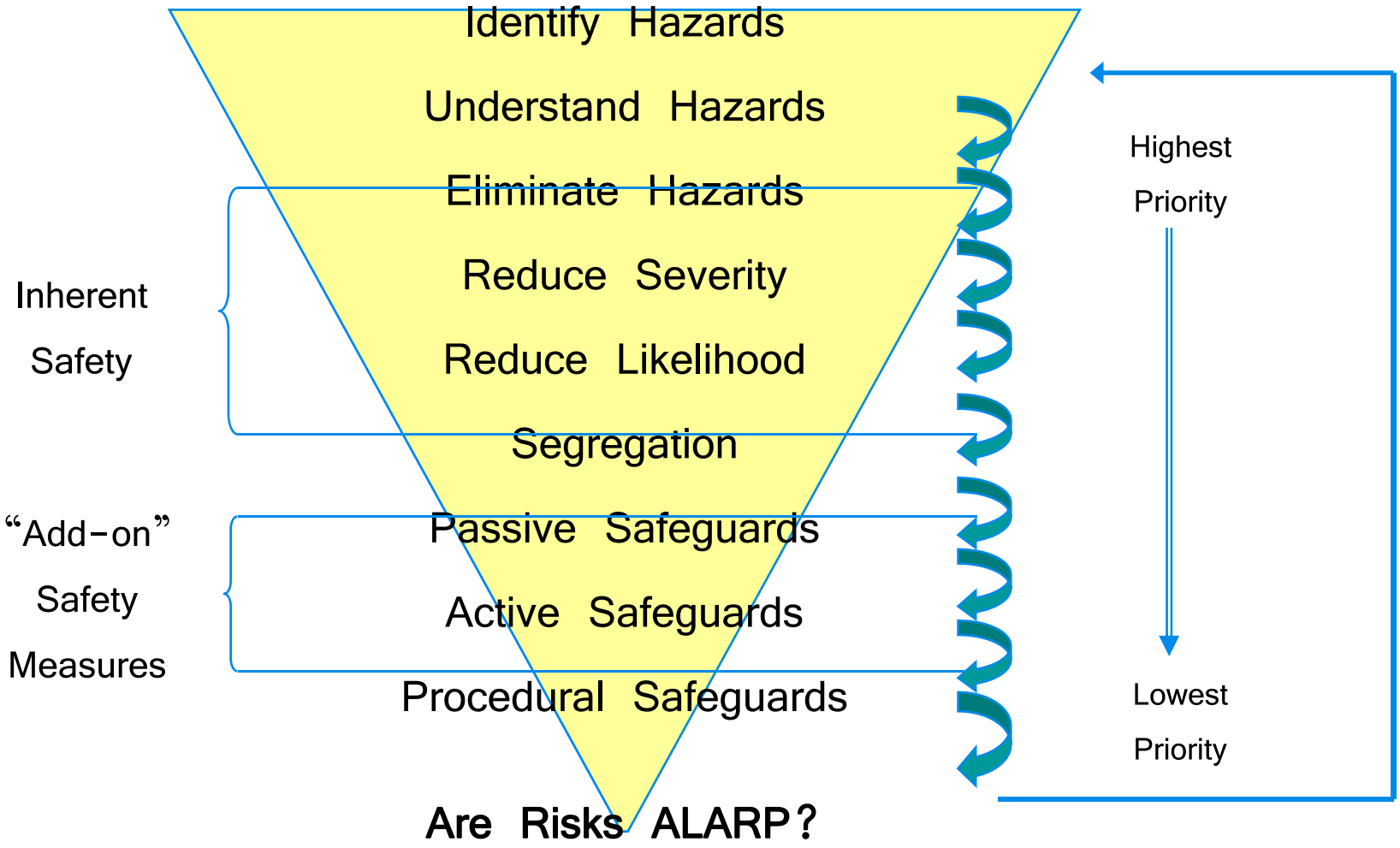
Typical Client's policy context

- Typical HSE commitment - no accidents, no harm to people, and no damage to the environment
  - Requires proactive process safety management including understanding the contribution that safety instrumented systems make in preventing hazards & managing integrity
- Process Safety / Integrity Management Standard
  - Elements for "Protective systems and/or devices are to be designed, installed, maintained and kept in service to provide adequate protection to the primary containment"
- Follow client's engineering technical practices on SIS

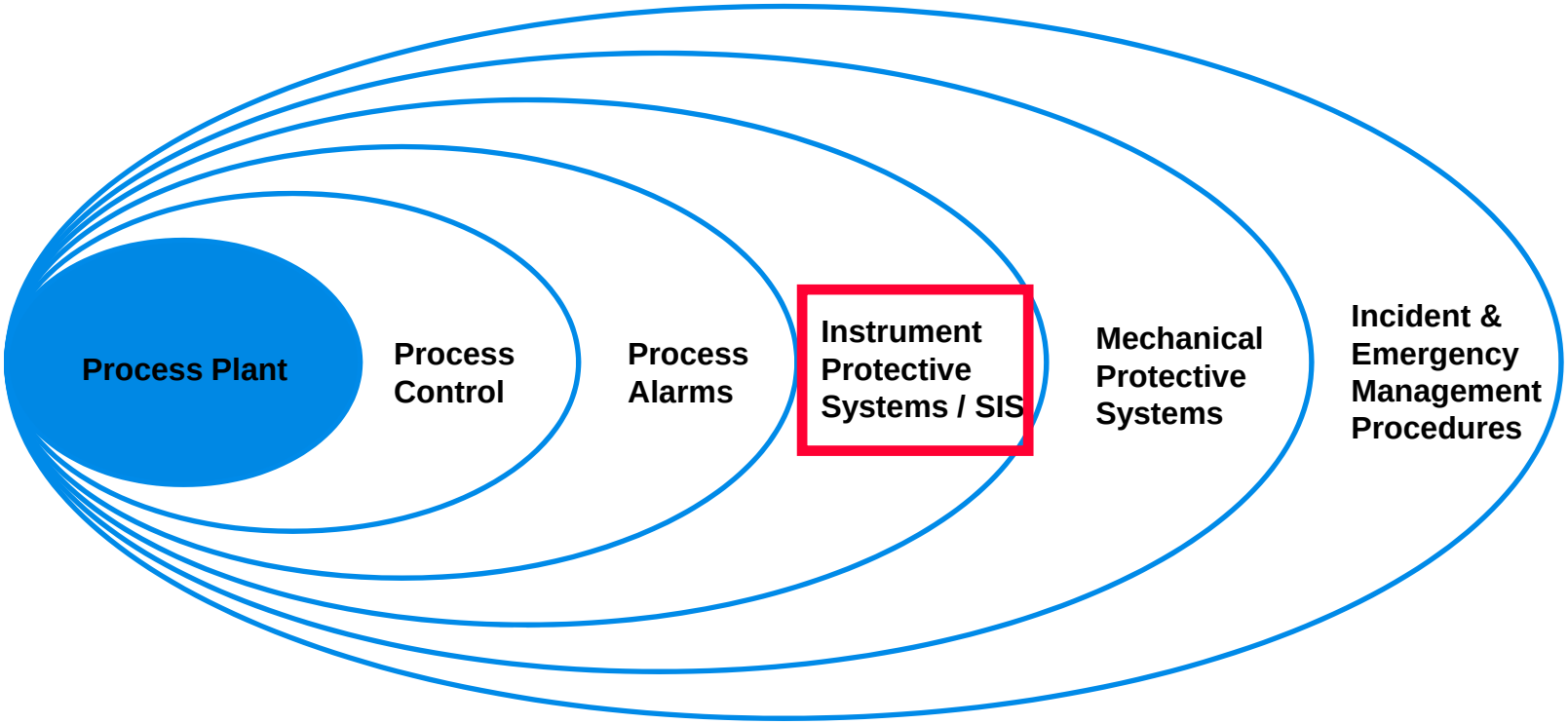
Engineering technical practices

- Based on IEC 61511-1 Functional safety – safety instrumented systems for the process industry sector
  - Which implements IEC 61508 Functional safety of electrical / electronic / programmable electronic safety-related systems
  - And includes input from ANSI/ISA S84.01 Application of Safety Instrumented Systems for the Process Industries

Hazard management process



Layers in hazard management



SIS Issues

1. How much reliance do we need to place on the protective system to address the process safety concerns for a given application **or** What integrity does it need to have What is its required performance standard
2. Engineer and maintain the system to achieve the required integrity or performance standard during its life

Other reasons for SIL assessment

- Some national regulatory authorities expect it from prudent operators
- Allows clients to focus testing effort on the minority of safety systems which are critical for managing safety, environmental or commercial risks and spend less effort on the majority which are not

Safety integrity levels (SIL)

- We need a recognised means of defining integrity
- Four levels defined in IEC 61508 / IEC 61511

Safety Integrity Level (SIL)	Probability of Failure on Demand (PFD)	Probability of Success on Demand	Risk Reduction Factor (RRF)
4 (NR)	10^{-4} - 10^{-5}	99.99 - 99.999%	10,000 - 100,000
3	10^{-3} - 10^{-4}	99.9 - 99.99%	1,000 - 10,000
2	10^{-2} - 10^{-3}	99 - 99.9%	100 - 1,000
1	10^{-1} - 10^{-2}	90 - 99%	10 - 100

NR = Not Recommended in ISA S84.01